UNITED STATES DISTRICT COURT

for the

District of Oregon

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

A blue Samsung cell phone, grey Samsung T7 SSD, red Samsung T7 SSD, silver and black HP laptop, and One Plus cell phone, as described in Attachment A

Case No. 3:25-mc-00678

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

A blue Samsung cell phone, a grey Samsung T7 SSD, a red Samsung T7 SSD, a silver and black HP laptop, and a One Plus cell phone, as further described in Attachment A hereto,

located in the _____ District of Oregon, there is now concealed *(identify the person or describe the property to be seized)*:

The information and items set forth in Attachment B hereto.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 2252A(a)(2)	Receipt of Child Pornography
18 U.S.C § 2252A(a)(5)(B)	Possession of and/or Access with Intent to View Child Pornography

The application is based on these facts:

See affidavit which is attached hereto and incorporated herein by this reference.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

H. Sheldon Clay, HSI Task Force Officer
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by Telephone at 11:25 a.m. *(specify reliable electronic means).*

Date: 06/10/2025

Stacie F. Beckerman
Judge's signature

City and state: Portland, Oregon

STACIE F. BECKERMAN, United States Magistrate Judge
Printed name and title

ATTACHMENT A

Property to Be Searched

The property to be searched is the following devices:

- a blue Samsung cell phone, model SM-A166U with no case;
- a grey Samsung T7 SSD portable storage drive;
- a red Samsung T7 SSD portable storage drive;
- a silver and black HP laptop computer; and
- a damaged One Plus brand cell phone

collectively, the **Subject Devices**, which are currently stored, in law enforcement possession, at the Newberg-Dundee Police Department in Yamhill County under Yamhill County Sheriff's Office Case #25YC1287.

ATTACHMENT B

Items to Be Seized

1. All records on the **Subject Devices** described in Attachment A that relate to violations of *Title 18 U.S.C. § 2252A(a)(2)* – Receipt of Child Pornography, and *18 U.S.C § 2252A(a)(5)(B)* – Possession of and/or Access with Intent to View Child Pornography, and collectively referred to as the **Target Offenses** including:

   a. Any records, documents, or materials, including correspondence, that pertain to any account, record, data, file, any other social media application or cloud-based storage, or any other business that can facilitate the **Target Offenses**.

   b. Any records, documents, or materials, including any communications or messages that pertain to any account, record, data, or any other internet-based chat application / video that can facilitate the **Target Offenses**.

   c. Any records, documents, or materials, including GPS location data, messages, calendar schedules, work schedule, and other data, that would identify the location of the digital device or the user of the digital device at a specific moment in time (for the purposes of comparing it when sexually explicit videos were made or where the user was located when they received the images / videos).

   d. Any records, documents, or materials, including correspondence, that pertain to the production, transportation, distribution, receipt, or possession of visual depictions of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256.

   e. All originals and copies (physical or digital) of visual depictions of minors

engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256.

f. Any motion pictures or digital video clips of visual depictions of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256; video recordings which are self-produced and pertain to sexually explicit images of minors; or video recordings of minors which may assist in the location of minor victims of child exploitation or child abuse.

g. Any records, documents, or materials which include offers to transmit, through interstate commerce by any means (including by computer), any visual depiction of a minor engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256.

h. Any records, documents, or materials relating to the production, reproduction, receipt, shipment, trade, purchase, or a transaction of any kind involving the transmission, through interstate commerce (including by computer), of any visual depiction of a minor engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256.

i. Any records, documents, or materials naming or identifying minors visually depicted while engaging in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256.

j. Any records of internet usage, including records containing screen names, usernames, and e-mail addresses, and identities assumed for the purposes of communication on the internet. These records include billing and subscriber

records, chat room logs, e-mail messages, and include electronic files in a computer and on other data storage media, including CDs or DVDs.

k. Any records, documents, or materials referring or pertaining to communications with others, whether in person, by telephone, or online, for the purpose of distributing or transporting child pornography, including chat logs, call logs, address book or contact list entries, and digital images or videos sent or received.

l. Any records, documents, or materials, including correspondence, that could assist in identifying the user of a particular cell phone, computer, or other digital device at a specific moment in time.

m. Information or evidence of any websites visited, photographs, videos, images, reports, definitions, stories, books, music, lyrics, emails, videos, messages, and or notes associated with child pornography or those who collect, disseminate, or trade in child pornography.

As used above, the terms "records," "documents," "programs," "applications," or "materials" include records, documents, programs, applications or materials created, modified or stored in any form including digital or electronic form.

Search Procedure

2. The examination of the device may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

3. The initial examination of the device will be performed within a reasonable

amount of time not to exceed 120 days from the date of execution of the warrant. If the government needs additional time to conduct this review, it may seek an extension of the time period from the Court within the original 120-day period from the date of execution of the warrant. The government shall complete this review within 180 days of the date of execution of the warrant. If the government needs additional time to complete this review, it may seek an extension of the time period from the Court.

4. If, at the conclusion of the examination, law enforcement personnel determine that particular files or file folders on the device or image do not contain any data falling within the scope of the warrant, they will not search or examine those files or folders further without authorization from the Court. Law enforcement personnel may continue to examine files or data falling within the purview of the warrant, as well as data within the operating system, file system, software application, etc., relating to files or data that fall within the scope of the warrant, through the conclusion of the case.

5. If an examination is conducted, and it is determined that the device does not contain any data falling within the ambit of the warrant, the government will return the device to its owner within a reasonable period of time following the search and will seal any image of the device, absent further authorization from the Court.

6. If the device contains evidence, fruits, contraband, or is an instrumentality of a crime, the government may retain the device as evidence, fruits, contraband, or an instrumentality of a crime or to commence forfeiture proceedings against the device and/or the data contained therein.

7. The government will retain a forensic image of the device for a number of

reasons, including proving the authenticity of evidence to be used at trial, responding to questions regarding the corruption of data, establishing the chain of custody of data, refuting claims of fabricating, tampering, or destroying data, and addressing potential exculpatory evidence claims where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third party.

DISTRICT OF OREGON, ss: AFFIDAVIT OF H. SHELDON CLAY

Affidavit in Support of an Application Under Rule 41 for a Warrant to Search and Seize Evidence Including Digital Evidence

I, H. Sheldon Clay, being duly sworn, do hereby depose and state as follows:

Introduction and Agent Background

1. I am a Task Force Officer with Homeland Security Investigations (HSI) since 2023, and I have been a sworn police officer in the State of Oregon since 2004. I hold Basic, Intermediate and Advanced police officer certifications with the Oregon Department of Public Safety Standards and Training. I have been assigned as a detective in various assignments since 2006. As a detective, I have worked person, property, drug, financial, computer/digital crimes. Since 2012, I have been assigned to work investigations involving digital evidence, including investigations involving child exploitation.

2. My formal law enforcement and related training consists of graduating from both a reserve police officer academy in 2004 and the Oregon Department of Public Safety Standards and Training (DPSST) Basic Police Class in 2005. I have over three thousand seven hundred (3700) hours of training recorded with the DPSST. Of that three thousand seven hundred hours, I have over 1300 hours of training in the acquisition, processing and investigation of digital evidence including; computers, mobile devices, GPS systems, credit card skimming devices, IOT devices, digital currency, drones, vehicle systems, and network intrusion response. I am a Certified Forensic Computer Examiner (CFCE) with the International Association of Computer Investigative Specialists (IACIS), I have a Global Information Assurance Certification (GIAC) in Advanced Smartphone Forensics (GASF), and I am both a Certified Cybercrime Investigator

(3CI) and a Certified Cybercrime Examiner (3CE) with the National White Collar Crime Center (NW3C).

3. During training, I learned how to conduct child exploitation investigations. Since then, I have been involved in many child exploitation investigations and have assisted federal and state agencies during their investigations. As such, I have become familiar with ways that child pornography is shared, distributed, and/or produced, including the use of various social media websites (Facebook, Twitter, Kik, Snapchat, Discord, Signal etc.), "cloud" based storage, and peer-to-peer (P2P) networks.

4. I have worked with officers and agents involved in numerous investigations involving the sexual exploitation of children or the distribution, receipt, and possession of child pornography. I have participated in searches of premises and assisted in gathering evidence pursuant to search warrants, including search warrants in multiple child pornography investigations. I have participated in interviews of persons who possess, distribute, and produce child pornography.

5. I submit this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the search and examination of a cell phone described as a blue in color Samsung, model SM-A166U with no case (**Device 1**), a grey in color Samsung T7 SSD portable storage drive (**Device 2**), a red in color Samsung T7 SSD portable storage drive (**Device 3**), a silver and black HP laptop computer (**Device 4**), and a damaged One Plus brand cell phone (**Device 5**) (collectively, the **Subject Devices**), as described in Attachment A hereto, and the extraction of electronically stored information from the **Subject Devices**, as described in Attachment B hereto. These five electronic devices were seized under

Yamhill County Sheriff's Office Case #25YC1287 and are currently stored, in law enforcement possession, at the Newberg-Dundee Police Department. As set forth below, I have probable cause to believe that the items set forth in Attachment B constitute evidence, contraband, fruits, and instrumentalities of violations of *Title 18 U.S.C. § 2252A(a)(2)* – Receipt of Child Pornography, and *18 U.S.C § 2252A(a)(5)(B)* – Possession of and/or Access with Intent to View Child Pornography, and collectively referred to as the **Target Offenses**.

6. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. The facts set forth in this affidavit are based on my own personal knowledge, knowledge obtained from other individuals during my participation in this investigation, including other law enforcement officers, interviews of witnesses, a review of records related to this investigation, communications with others who have knowledge of the events and circumstances described herein, and information gained through my training and experience.

Applicable Law

7. *Title 18, United States Code, Section 2252A(a)(2)* makes it a crime to knowingly receive or distribute any child pornography using any means or facility of interstate or foreign commerce, or that has been mailed, shipped, or transported in or affecting interstate or foreign commerce by any means, including by computer.

8. *Title 18, United States Code, Section 2252A(a)(5)(B)* makes it a crime to knowingly possess or access with intent to view child pornography that has been mailed, shipped, or transported in or affecting interstate or foreign commerce by any means, including by

computer, or that was produced using materials that were mailed, shipped, or transported in or affecting interstate or foreign commerce by any means, including by computer.

9. The term "child pornography" is defined in 18 U.S.C. § 2256(8). "Child pornography," as defined in 18 U.S.C. § 2256(8), includes any visual depiction of a child under the age of 18 years engaging in sexually explicit conduct. "Sexually explicit conduct" is defined in 18 U.S.C. § 2256(2) and includes sexual intercourse, whether genital-genital, oral-genital, anal-genital, or oral-anal, whether between members of the same or opposite sex; bestiality; masturbation; sadistic or masochistic abuse; and the lascivious exhibition of the genitals, anus, or pubic area of any person.

Statement of Probable Cause

YCSO Contacts HSI regarding digital devices seized in CSAM investigation

10. On May 20, 2025, I spoke with detectives from the Yamhill County Sheriff's Office (YCSO) regarding **Joshua David STORM**. I learned from the detectives that on May 18, 2025, YCSO received information from **Witness 1**, a dating partner of **STORM**, who reported that **STORM** had pictures and videos of child pornography, including images of children approximately 5 years old, on his cell phone stored in the camera roll. **Witness 1** stated they had the passcode for **STORM's** cell phone and had accessed **STORM's** cell phone without his knowledge. **Witness 1** stated that they viewed some of the child pornography on the phone, but not all of it due to there being such a large amount. While viewing the contents of **STORM's** phone, **Witness 1** used their phone to record some of the images of child pornography on **STORM's** cell phone for the purpose of showing law enforcement. **Witness 1** later showed the images to a YCSO deputy, who confirmed the images included videos and photos of adult men

having vaginal and oral sexual intercourse with female children who appeared to be under the age of 12. Additionally, **Witness 1** stated they saw an unfamiliar messaging application called "Potato" on **STORM's** cell phone.

11. A YCSO Deputy and Detective contacted **STORM** at his place of employment, Ruby's Mart and Tobacco, 2411 NE McDonald Ln, McMinnville, Oregon, to interview him and seize his cell phone. When the deputy and detective contacted **STORM** and advised him they needed to speak with him and seize his phone, **STORM** stepped back and began arguing with the Detective about handing over his phone. **STORM** was given multiple warnings to hand over his phone or force may be used to secure it. **STORM** did not comply with the Deputies' commands and physically resisted being detained. While **STORM** was fighting with the Deputy and Detective over his cell phone, the Deputy attempted twice to deploy his Taser on **STORM,** but **STORM** pulled out the Taser probes and fled the store on foot with his cell phone.

12. The Deputy pursued **STORM** on foot for several blocks, at one point losing sight of **STORM.** A citizen who was driving in the area saw the Deputy pursing **STORM** and began following **STORM** in his vehicle. The Citizen blocked **STORM's** path with his vehicle and **STORM** was detained by the Deputy. The Citizen then advised the Deputy that **STORM** had discarded his cell phone in a nearby trash can. The Deputy retrieved **STORM's** cell phone (**Device 1**) from the trash can.

13. **STORM** was lodged at the Yamhill County Jail on state charges and the Detective obtained a seizure warrant and later a search warrant for **STORM's** cell phone. YCSO personal attempted to process **STORM's** cell phone with available digital forensics tools, but

were unsuccessful in obtaining a forensic copy of the device due to the device's security features, even when using the passcode.

14. On May 19, 2025, **Witness 1** again contacted YCSO and advised they had found two Samsung portable solid state (SSD) storage drives in **STORM's** backpack, one a Grey in color Samsung T7 1 Terabyte SSD (**Device 2**) and the other a red in color Samsung T7 500 Gigabyte SSD (**Device 3**). **Witness 1** stated they had connected the red Samsung SSD to their computer and saw it contained child pornography. **Witness 1** turned over both of the Samsung drives to YCSO.

15. A YCSO detective obtained a seizure warrant and later a Search Warrant from the Yamhill County Circuit Court to examine the Samsung Drives for images or videos of child pornography. YCSO brought **Devices 1, 2, and 3** to the Newberg-Dundee Police Department Digital Forensics Lab on May 20, 2025. On May 22, 2025, I used digital forensics tools to conduct a preview of images and pictures on the **Devices 1, 2, and 3** under the limited scope of the Circuit Court-issued Search Warrants.

16. On June 4, 2025, I learned that Witness 1 had located additional electronic items belonging to **STORM** in a storage bin. After locating the items on June 3, 2025, **Witness 1** contacted YCSO to turn over the electronic items. **Witness 1** met with a YCSO deputy who collected the electronics and placed them into evidence. On June 4, 2025, I met with a YCSO Detective who showed me the items packaged in clear evidence bags. Of the items, I identified a silver and black HP laptop computer (**Device 4**) and a One Plus brand cell phone with significant physical damage including a shattered screen, bulged battery and punctured rear cover (**Device 5**) that could contain digital evidence. The other electronic items consisted of chargers, adapters

and a Nintendo game card. I brought **Device 4** and **Device 5** to the Newberg-Dundee Police Department Digital Forensics lab.

17. The **Subject Devices** are currently in storage at the Newberg-Dundee Police Department Digital Forensics Lab. In my training and experience, I know that the **Subject Device**s have been stored in a manner in which their contents are, to the extent material to this investigation, in substantially the same state as they were when the **Subject Devices** first came into the possession of authorities.

18. I know, based on my training and experience, and based on conversations I have had with others who investigate child exploitation offenses, that people who have a sexual interest in children, including persons who collect and trade in child pornography, often receive sexual gratification from images and video clips depicting the sexual exploitation of children. Such persons maintain their collections of child pornography in safe, secure, and private locations, such as their residence or vehicle, and on computers, cell phones, and digital storage media under their direct control. Such persons often maintain their collections, which are considered prized possessions, for long periods of time, and prefer not to be without their collections for any prolonged period. In some recent cases, however, some persons with a sexual interest in children have been found to download and delete child pornography on a cyclical and repetitive basis, rather than storing a collection of child pornography indefinitely.

19. I also know from my training and experience that many people who download child pornography from the Internet, and those who collect child pornography, frequently save images and videos of child pornography on their computers and cell phones and/or transfer copies to other devices and storage media, including cloud storage accounts, external hard drives,

thumb drives, flash drives, SD cards, and CDs or DVDs. Moreover, it is common in child pornography investigations to find child pornography on multiple devices and/or storage media located in suspects' homes, rather than on a single device.

20. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. *Wireless telephone*. A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books"; sending, receiving, and storing text messages and email; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. *Digital camera*. A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage

medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. *Portable media player*. A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. *GPS*. A GPS navigation device uses the Global Positioning System to display its current location. It often contains historical records of the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated as "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude

with a high level of precision.

h. *Storage medium*. A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

Based on my training and experience, I use the following technical terms to convey the following meanings:

a. *Wireless telephone*. A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books"; sending, receiving, and storing text messages and email; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. *Digital camera*. A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be

retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. *Portable media player*. A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. *GPS*. A GPS navigation device uses the Global Positioning System to display its current location. It often contains historical records of the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated as "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that

antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. *Storage medium*. A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

21. Based on my training, experience, and research I know that the **Subject Devices** have amongst them various capabilities that allow them to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and storage media. In my training and experience, examining data stored on devices of these types can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

22. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

23. As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant but also forensic evidence that establishes how the **Subject Devices** were used, the purpose of their use, who used it, and when. There is probable cause to believe that this forensic electronic evidence will be on the **Subject Devices** because, based on my knowledge, training, and experience, I know:

a. Data on the device can provide evidence of a file that was once on the device but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph

that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, email programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, email, email address books, "chat," instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the device at a relevant time. Further, forensic evidence on a device can show how and when the device was accessed or used. Such "timeline" information allows the forensic analyst and investigators to understand the chronological context of access, use, and events relating to the crime under investigation. This "timeline" information may tend to either inculpate or exculpate the device user. Last, forensic evidence on a device may provide relevant insight into the device user's state of mind as it relates to the offense under investigation. For example, information on a device may indicate the user's motive and intent to commit a crime (e.g., relevant web searches occurring before a crime indicating a plan to commit the same),

consciousness of guilt (e.g., running a "wiping program" to destroy evidence on the device or password protecting or encrypting such evidence in an effort to conceal it from law enforcement), or knowledge that certain information is stored on a computer (e.g., logs indicating that the incriminating information was accessed with a particular program).

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a device is evidence may depend on other information stored on the device and the application of knowledge about how a device behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. I know that when an individual uses an electronic device to commit a crime, such as to obtain child pornography, the electronic device will generally serve both as an instrumentality for committing the crime and as a storage medium for evidence of the crime.

From my training and experience, I believe that an electronic device used to commit a crime of this type may contain: data that is evidence of how the electronic device was used; data that was sent or received; and other records that indicate the nature of the offense.

24. *Nature of examination*. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

25. The initial examination of the device will be performed within a reasonable amount of time not to exceed 120 days from the date of execution of the warrant. If the government needs additional time to conduct this review, it may seek an extension of the time period from the Court within the original 120-day period from the date of execution of the warrant. The government shall complete this review within 180 days of the date of execution of the warrant. If the government needs additional time to complete this review, it may seek an extension of the time period from the Court.

26. If, at the conclusion of the examination, law enforcement personnel determine that particular files or file folders on the device or image do not contain any data falling within the scope of the warrant, they will not search or examine those files or folders further without authorization from the Court. Law enforcement personnel may continue to examine files or data falling within the purview of the warrant, as well as data within the operating system, file system, software application, etc., relating to files or data that fall within the scope of the warrant, through the conclusion of the case.

27. If an examination is conducted, and it is determined that the device does not contain any data falling within the ambit of the warrant, the government will return the device to its owner within a reasonable period of time following the search and will seal any image of the device, absent further authorization from the Court.

28. If the device contains evidence, fruits, contraband, or is an instrumentality of a crime, the government may retain the device as evidence, fruits, contraband, or an instrumentality of a crime or to commence forfeiture proceedings against the device and/or the data contained therein.

29. The government will retain a forensic image of the device for a number of reasons, including proving the authenticity of evidence to be used at trial, responding to questions regarding the corruption of data, establishing the chain of custody of data, refuting claims of fabricating, tampering, or destroying data, and addressing potential exculpatory evidence claims where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third party.

30. *Manner of execution*. Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

Conclusion

31. Based on the foregoing, I have probable cause to believe that the **Subject Devices** described in Attachment A contain evidence, contraband, and instrumentalities of violations of *Title 18 U.S.C. § 2252A(a)(2)* – Receipt of Child Pornography, and *18 U.S.C § 2252A(a)(5)(B)* –

Possession of and/or Access with Intent to View Child Pornography (**Target Offenses**), as set forth in Attachment B. I therefore request that the Court issue a warrant authorizing a search of the **Subject Devices** described in Attachment A for the items listed in Attachment B and the seizure and examination of any such items found.

32. Prior to being submitted to the Court, this affidavit, the accompanying application, and the requested search warrant were all reviewed by Assistant United States Attorney Mira Chernick. I was informed that it is AUSA Chernick's opinion that the affidavit and application are legally and factually sufficient to establish probable cause to support the issuance of the requested warrant.

By phone pursuant to Fed R. Crim. P. 4.1
H. SHELDON CLAY
Task Force Officer, HSI

Subscribed and sworn in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone at 11:25 a.m. on June 10, 2025.

HONORABLE STACIE F. BECKERMAN
UNITED STATES MAGISTRATE JUDGE